

**This Page Is Inserted by IFW Operations  
and is not a part of the Official Record**

## **BEST AVAILABLE IMAGES**

**Defective images within this document are accurate representations of the original documents submitted by the applicant.**

**Defects in the images may include (but are not limited to):**

- **BLACK BORDERS**
- **TEXT CUT OFF AT TOP, BOTTOM OR SIDES**
- **FADED TEXT**
- **ILLEGIBLE TEXT**
- **SKEWED/SLANTED IMAGES**
- **COLORED PHOTOS**
- **BLACK OR VERY BLACK AND WHITE DARK PHOTOS**
- **GRAY SCALE DOCUMENTS**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-164656

(43)Date of publication of application : 19.06.1998

(51)Int.Cl.

H04G 7/38  
H04L 9/08  
H04L 9/14  
H04M 1/66  
H04M 3/22

(21)Application number : 08-314733

(71)Applicant : HITACHI LTD

(22)Date of filing : 26.11.1996

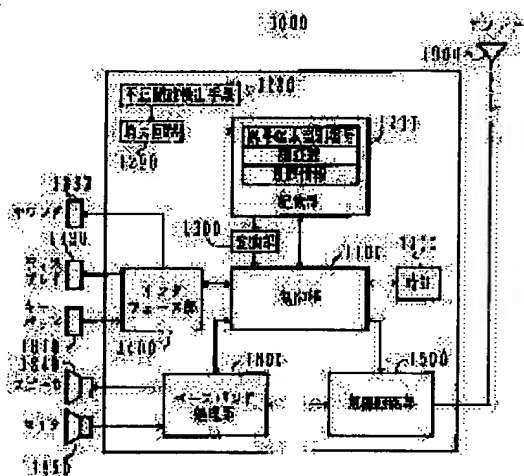
(72)Inventor : KOIDE AYUMI  
KITAMURA YOICHI

(54) PORTABLE TERMINAL, MANAGING CENTER THEREFOR AND SUPERVISORY AND CONTROL PART THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a portable terminal, portable terminal managing center and supervisory and control part of the terminal hardly performing unauthorized speaking by generating a new certificate key based on a certificate key and history information, using the new certificate key, converting certificate data sent from a base station into certificate response data and transferring the data to the base station.

SOLUTION: A control part 1100 of portable terminal 1000 performs entire control or history information calculation/storage, etc. A storage part 1200 stores portable terminal identification numbers, fixed certificate keys and history information or the like of respective registered portable terminals. Based on the fixed certificate keys and history information stored in the storage part 1200, a converting part 1300 generates the new certificate key. In the case, since the history information is successively reloaded at the time point of speaking end, the newly generated certificate key becomes a successively variable certificate key so as to be hardly illegally acquired.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-164656

(43) 公開日 平成10年(1998)6月19日

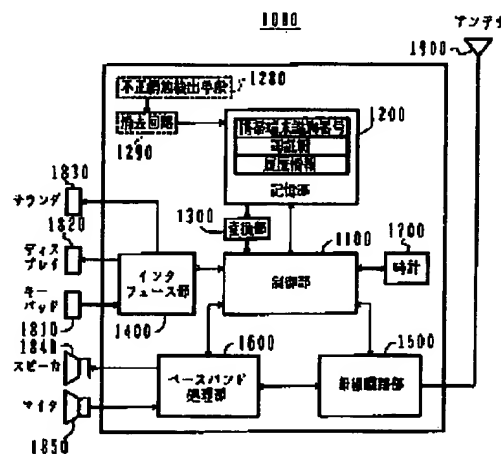
| (51) Int.Cl. <sup>4</sup>     | 識別記号             | P I      |   |
|-------------------------------|------------------|----------|---|
| H 0 4 Q                       | 7/38             | H 0 4 B  | 7/28 1 0 9 R                                      |
| H 0 4 L                       | 9/08             | H 0 4 M  | 1/66 B  |
|                               | 9/14             |          | 3/22 Z  |
| H 0 4 M                       | 1/66             | H 0 4 L  | 9/00 6 0 1 B                                      |
|                               | 3/22             |          | 6 4 1   |
| 審査請求 未請求 請求項の数 7 O L (全 11 頁) |                  |          |   |
| (21) 出願番号                     | 特願平8-314733      | (71) 出願人 | 000005108<br>株式会社日立製作所<br>東京都千代田区神田駿河台四丁目6番地      |
| (22) 出願日                      | 平成8年(1996)11月28日 | (72) 発明者 | 小出 歩<br>神奈川県横浜市戸塚区戸塚町216番地 株<br>式会社日立製作所情報通信事業部内  |
|                               |                  | (72) 発明者 | 北村 洋一<br>神奈川県横浜市戸塚区戸塚町216番地 株<br>式会社日立製作所情報通信事業部内 |
|                               |                  | (74) 代理人 | 弁理士 春日 謙  |

(54) 【発明の名称】 携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部

(57) 【要約】

【課題】 本発明の目的は、不正通話の行い難い携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部を提供することにある。

【解決手段】 携帯端末1000は、携帯端末識別番号と携帯端末毎に予め与えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部1200と、この記憶部1200に記憶された認証鍵と履歴情報に基づいて新たな認証鍵を生成する変換部1300と、この変換部1300によって生成された新たな認証鍵を用いて、基地局2100から送られてきた認証データを認証応答データに変換する制御部1100とから構成されている。



(2)

特開平10-164656

1

【特許請求の範囲】

【請求項1】 携帯端末識別番号と携帯端末毎に予め与えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部と、

この記憶部に記憶された上記認証鍵と上記履歴情報に基づいて新たな認証鍵を生成する変換部と、

この変換部によって生成された新たな認証鍵を用いて、基地局から送られてきた認証データを認証応答データに変換する制御部とを備え、

この制御部で変換された認証応答データを上記基地局に転送することを特徴とする携帯端末、

【請求項2】 請求項1記載の携帯端末において、

上記記憶部に記憶されている履歴情報は、過去の通話回数、過去の通話開始時間、過去の通話終了時間、過去の通話時間、及び過去の通話位置からなることを特徴とする携帯端末、

【請求項3】 請求項1記載の携帯端末において、さらに、

上記記憶部を内蔵する筐体の不正開放を検出する不正開放検出手段を備え、

この不正開放検出手段による筐体の不正開放の検出信号に基づいて、上記記憶部の記憶内容を消去することを特徴とする携帯端末、

【請求項4】 携帯端末識別番号と携帯端末毎に予め与えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部と、

この記憶部に記憶された上記認証鍵と上記履歴情報に基づいて新たな認証鍵を生成する変換部と、

この変換部によって生成された新たな認証鍵を用いて、認証データを認証応答データに変換するとともに、携帯端末から送られてきた認証応答データと比較して、両者が一致した場合に、通話を許可する制御部とを備えたことを特徴とする携帯端末の管理センタ、

【請求項5】 請求項4記載の携帯端末の管理センタにおいて、

上記記憶部に記憶されている履歴情報は、過去の通話回数、過去の通話開始時間、過去の通話終了時間、過去の通話時間、及び過去の通話位置からなることを特徴とする携帯端末の管理センタ、

【請求項6】 携帯端末毎に通話料金の上限値を記憶する記憶部と、

この記憶部に記憶された上記通話料金の上限値を越えた場合に、管理センタに携帯端末の停止命令のコマンドを送る制御部とを備えたことを特徴とする携帯端末の監視制御部、

【請求項7】 携帯端末の過去の通話開始時間と過去の通話位置を記憶する記憶部と、

この記憶部に記憶された過去の通話開始時間と過去の通話位置の情報に基づいて、一定時間内に、通話位置が前回の通話位置から予め設定しておいた距離以上である場

2

合、管理センタに、携帯端末の停止命令のコマンドを送る制御部とを備えたことを特徴とする携帯端末の監視制御部、

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部に係り、特に、クローニング対策を講じた携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部に関する。

【0002】

【従来の技術】携帯端末を用いる無線通信システムにおいては、無線区間で他人の携帯端末のID等の識別番号を盗み出し、自身の携帯端末に盗み出したID等の識別番号を書き込むことによって他人に成りすまし、他人の課金で携帯端末を利用するクローニングによる被害が問題になっている。

【0003】このような不正な携帯端末による使用を防止するため、従来は、例えば、斉藤、立川著「移動通信ハンドブック」、オーム社、p. 152に記載されているように、各携帯端末毎に、予め携帯端末に固有の認証鍵を割り当てるようにしていた。

【0004】携帯端末は、基地局に接続するため、基地局に対してサービス要求を送出する。基地局は、認証を行うために必要な認証用乱数Rを生成し、認証用乱数を携帯端末に伝送する。携帯端末は、認証用乱数を携帯端末毎に割り当てられている認証鍵を用いて、認証応答データに変換し、基地局に送り返す。基地局は、携帯端末から送られてきた認証応答データと基地局内で予め求めておいた認証応答データと比較して、両者が一致する場合にのみ、接続を許可するようにしている。正当な携帯端末でない場合には、携帯端末毎に対応する認証鍵を持っていないので、認証応答データへの変換が正しく行われないため、基地局は接続を拒否することになる。このような認証方法を用いることによって、基地局は、不正な携帯端末をチェックするようにしているものである。

【0005】

【発明が解決しようとする課題】従来の端末認証は、各携帯端末毎に、予め割り当てられていた固有の認証鍵を用いるため、この認証鍵が知られてしまった場合、別の携帯端末のROM等の記憶装置に認証鍵をインプットするだけで、クローン携帯端末を簡単に作成できる。従って、このようなクローン携帯端末を使用して、他人を装って、他人の料金で不正通話を行う場合が生じるという問題があった。

【0006】本発明の目的は、不正通話の行い難い携帯端末及び携帯端末の管理センタ及び携帯端末の監視制御部を提供することにある。

【0007】

【課題を解決するための手段】上記目的を達成するために、本発明は、携帯端末識別番号と携帯端末毎に予め与

(3)

特開平10-164656

えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部と、この記憶部に記憶された上記認証鍵と上記履歴情報に基づいて新たな認証鍵を生成する変換部と、この変換部によって生成された新たな認証鍵を用いて、基地局から送られてきた認証データを認証応答データに変換する制御部とを備え、この制御部で変換された認証応答データを上記基地局に転送するようにしたものであり、かかる構成により、認証鍵が逐次更新されるため、不正使用を行い難くなるものである。

【0008】上記携帯端末において、好ましくは、上記記憶部に記憶されている履歴情報は、過去の通話回数、過去の通話開始時間、過去の通話終了時間、過去の通話時間、及び過去の通話位置から構成したものである。

【0009】上記携帯端末において、好ましくは、さらに、上記記憶部を内蔵する筐体の不正開放を検出する不正開放検出手段を備え、この不正開放検出手段による筐体の不正開放の検出信号に基づいて、上記記憶部の記憶内容を消去するようにしたものである。

【0010】上記目的を達成するために、本発明は、携帯端末識別番号と携帯端末毎に予め与えられている認証鍵と携帯端末の過去の使用状況を示す履歴情報とを記憶する記憶部と、この記憶部に記憶された上記認証鍵と上記履歴情報に基づいて新たな認証鍵を生成する変換部と、この変換部によって生成された新たな認証鍵を用いて、認証データを認証応答データに変換するとともに、携帯端末から送られてきた認証応答データと比較して、両者が一致した場合に、通話を許可する制御部とを備えるようにしたものであり、かかる構成により、認証鍵が逐次更新されるため、不正使用を行い難くなるものである。

【0011】上記携帯端末において、好ましくは、上記記憶部に記憶されている履歴情報は、過去の通話回数、過去の通話開始時間、過去の通話終了時間、過去の通話時間、及び過去の通話位置から構成したものである。

【0012】上記目的を達成するために、本発明は、携帯端末毎に通話料金の上限値を記憶する記憶部と、この記憶部に記憶された上記通話料金の上限値を越えた場合に、管理センタに携帯端末の停止命令のコマンドを送る制御部とを備えるようにしたものであり、かかる構成により、通話料金が上限値を越えたか否かに基づいて、容易に不正使用を判断し得るものとなる。

【0013】上記目的を達成するために、本発明は、携帯端末の過去の通話開始時間と過去の通話位置を記憶する記憶部と、この記憶部に記憶された過去の通話開始時間と過去の通話位置の情報に基づいて、一定時間内に、通話位置が前回の通話位置から予め設定しておいた距離以上である場合、管理センタに、携帯端末の停止命令のコマンドを送る制御部とを備えるようにしたものであり、かかる構成により、通話位置と時間の情報により、

容易に不正使用を判断し得るものとなる。

【0014】

【発明の実施の形態】以下、図1～図5を用いて、本発明の一実施形態による携帯電話システムについて説明する。最初に、図1を用いて、本発明の一実施形態による携帯電話システムの全体構成について説明する。図1は、本発明の一実施形態による携帯電話システムのブロック図である。

【0015】携帯電話システムは、複数の携帯端末1000-1、1000-2、1000-3と、複数の基地局2100-1、2100-2、2100-3と、交換制御局2200と、管理センタ2300と、監視制御部2400とから構成されている。

【0016】複数の携帯端末1000-1、1000-2、1000-3は、それぞれ、移動可能であり、通話時には、最も近接する基地局2100-1、2100-2、2100-3との間で、無線通信により接続される。交換制御局2200は、一方では、公衆網3100を介して複数の電話機3200や他の通信機器に接続され、他方では、基地局2100-1、2100-2、2100-3に接続されており、所望の携帯端末1000-1、1000-2、1000-3と所望の電話機3200間の交換制御を行うものである。

【0017】管理センタ2300は、その内部に認証手段を備えており、この認証手段は、携帯端末1000-1、1000-2、1000-3が正当な使用であるか否かを判定を行い、正当な使用であると判定された場合には、交換制御局2200に対して接続を許可し、不正使用であると判定された場合には、交換制御局2200に対して接続を拒否するものである。管理センタ2300の詳細構成については、図2を用いて後述する。

【0018】監視制御部2400は、各携帯端末1000-1、1000-2、1000-3の使用状況を監視しており、管理センタ2300とは異なる方式により、不正使用のチェックを行い、不正使用であると判断される場合には、交換制御局2200に対して接続を拒否するようにしている。監視制御部2400の詳細構成については、図6を用いて後述する。

【0019】次に、図2を用いて、本発明の一実施形態による携帯電話システムにおいて用いる携帯端末1000の構成について説明する。図2は、本発明の一実施形態による携帯電話システムにおいて用いる携帯端末のブロック図である。

【0020】携帯端末1000は、制御部1100と、記憶部1200と、変換部1300と、インタフェース部1400と、無線回路部1500と、ベースバンド処理部1600と、時計1700とから構成されている。

【0021】制御部1100は、携帯端末1000の全体の制御や、履歴情報算出・格納等を行うものである。記憶部1200は、携帯端末識別番号と、登録されてい

(4)

特開平10-164656

5

る携帯端末個々の固定の認証鍵と、履歴情報とを記憶している。ここで、履歴情報については、図4を用いて後述するが、例えば、登録されている携帯端末個々の過去の通話回数、過去の通話相手先電話番号、過去の通話開始時間、過去の通話終了時間、過去の通話時間、過去の通話位置から構成されている。また、記憶部1200は、制御データや制御手順の情報も記憶している。

【0022】変換部1300は、記憶部1200に記憶されている固定の認証鍵と履歴情報に基づいて、本実施形態による新しい認証鍵を生成する。ここで、履歴情報は、通話の終了時点で、逐次書き換えられるものであるため、新たに生成される認証鍵は、逐次可変の認証鍵となる。従って、従来のような固定の認証鍵の場合に比べて、他人によって不正に取得されにくいものとなり、不正通話もしにくくなるものである。

【0023】インタフェース部1400は、携帯端末1000の入出力部を構成するキー入力を行うキーパッド1810と、表示出力を行うディスプレイ1820と、着信音等を出力するサウンダ1830と、制御部1100の間の入出力を制御する。

【0024】無線回路部1500は、アンテナ1900によって受信した無線信号を処理する高周波回路部である。ベースバンド処理部1600は、無線回路部1500から送られてくる信号を低周波信号に復調して、スピーカ1850から音声信号を出力する。また、マイク1860から入力された音声信号は、ベースバンド処理部1600によって変調され、無線回路部1500によって高周波信号に変換され、アンテナ1900を介して放射される。

【0025】時計1700は、時間を計測し、記憶部1200に記憶される履歴情報の中の過去の通話開始時間、過去の通話終了時間、過去の通話時間等の時間に関する情報の基準となる時間信号を発生している。

【0026】なお、各構成要素は、例えば、DSP、CPU、ROM、RAM各種CMOS等の電子デバイスにて実現可能である。

【0027】次に、図3を用いて、本発明の一実施形態による携帯電話システムにおいて用いる管理センタ2300の構成について説明する。図3は、本発明の一実施形態による携帯電話システムにおいて用いる管理センタのブロック図である。

【0028】管理センタ2300は、制御部2310と、記憶部2320と、変換部2330と、インタフェース部2340と、時計2350とから構成されている。

【0029】制御部2310は、管理センタ2300の全体の制御や、履歴情報算出・格納等を行うものである。記憶部2320は、図2に示した携帯端末1000の記憶部1200と同様に、携帯端末識別番号と、登録されている携帯端末個々の固定の認証鍵と、履歴情報と

6

を記憶している。ここで、履歴情報は、例えば、登録されている携帯端末個々の過去の通話回数、過去の通話相手先電話番号、過去の通話開始時間、過去の通話終了時間、過去の通話時間、過去の通話位置から構成されている。しかしながら、携帯端末1000の記憶部1200に記憶されている情報は、個々の携帯端末1000の情報だけであるのに対して、管理センタ2300の記憶部2330には、全ての携帯端末1000-1、1000-2、1000-3、…の携帯端末識別番号と携帯端末個々の固定の認証鍵と履歴情報の全てが記憶されている。履歴情報は、個々の携帯端末1000-1、1000-2、1000-3、…の通話の終了時点で、逐次書き換えられるものであり、携帯端末1000の記憶部1200に記憶される履歴情報と、管理センタ2300の記憶部2320に記憶される履歴情報は、同じものとなっている。また、記憶部2320は、制御データや制御手順の情報も記憶している。

【0030】変換部2330は、記憶部2320に記憶されている固定の認証鍵と履歴情報に基づいて、本実施形態による新しい認証鍵を生成する。

【0031】インタフェース部2340は、交換制御局2200との接続を制御する。時計2350は、時間を計測し、記憶部2320に記憶される履歴情報の中の過去の通話開始時間、過去の通話終了時間、過去の通話時間等の時間に関する情報の基準となる時間信号を発生している。

【0032】なお、各構成要素は、例えば、DSP、CPU、ROM、RAM各種CMOS等の電子デバイスにて実現可能である。

【0033】次に、図4を用いて、本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタ内部の変換部の構成について説明する。図4は、本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタ内部の変換部のブロック図である。なお、ここでは、携帯端末1000の中の変換部1300を例にとって説明するが、管理センタ2300の中の変換部2320の構成も同様である。

【0034】変換部1300には、図2に示した記憶部1200から履歴情報と固定の認証鍵が入力する。履歴情報としては、携帯端末の過去の通話回数1210と、過去の通話相手先電話番号1220と、過去の通話開始時間1230と、過去の通話終了時間1240と、過去の通話時間1250と、過去の通話位置1260とから構成されているものとする。

【0035】携帯端末の過去の通話回数1210は、携帯端末が使用可能になってからの過去の全通話回数であり、Nビットの情報で表される。制御部1100は、通話毎に最新の通話回数1210をインクリメントし、記憶部1200に格納する。過去の通話相手先電話番号1220は、通話毎に交換制御局2200（図1）より

50

(5)

特開平10-164656

7

転送されてくる情報であり、N2ビットの情報で表される。制御部1100は、通話毎に最新の通話相手先電話番号1220を記憶部1200に格納する。

【0036】過去の通話開始時間1230、通話終了時間1240、及び通話時間1250は、通話開始・終了時に時計1700で得られる通話接続年月日・時刻情報であり、それぞれN3ビット、N4ビット、N5ビットの情報で表される。制御部1100は、通話毎に最新の過去の通話開始時間1230、通話終了時間1240、通話時間1250を記憶部1200に格納する。

【0037】過去の通話位置1260は、携帯端末を使った位置特定システムによって得られる位置情報であり、N6ビットの情報で表される。PHSを使う位置特定システムについては、例えば、日経エレクトロニクス、1996.7.15、(no.666)に記載されている。図1に示した特定の携帯端末1000-1と、複数の基地局2100A、2100B、2100Cの間の接続は、携帯端末1000-1からの信号を受信した複数の基地局2100A、2100B、2100Cの信号強度を、交換制御部2200が判断して、最も電界強度の大きな基地局との間で成立するように制御される。従って、もし、基地局2100Aが受信する携帯端末1000-1から電界強度が最も大きいときには、基地局2100Aが交換制御部2200によって選択される。携帯端末1000が移動する際には、どの移動に応じて基地局2100の順次最も電界強度の大きい基地局に切り換えられる。従って、通話終了時において、接続されていた基地局2100を、過去の通話位置1260として、制御部1100は、通話毎に最新の過去の通話位置1260を記憶部1200に格納する。

【0038】さらに、固定の認証鍵1270は、N7ビットで表されるものとする。

【0039】ここで、携帯端末の過去の通話回数1210(N1ビット)と、過去の通話相手先電話番号1220(N2ビット)と、過去の通話開始時間1230(N3ビット)と、通話終了時間1240(N4ビット)と、通話時間1250(N5ビット)と、過去の通話位置1260(N6ビット)と、固定の認証鍵1270(N7ビット)の合計ビット数を、128ビットとする。この128ビットのパラレルデータが、変換部1300に取り込まれる。

【0040】変換部1300は、2個の疑似乱数発生回路1310、1320と、論理和回路1330とから構成されている。疑似乱数発生回路1310、1320は、例えば、岡本尊、「暗号理論入門」、共立出版に記載されているようなフィードバックシフトレジスタによる疑似乱数発生回路である。疑似乱数発生回路1310には、記憶部1200から取り込まれた128ビットのデータの内の下位の64ビットのパラレルデータが初期設定される。また、疑似乱数発生回路1320には、記

8

憶部1200から取り込まれた128ビットのデータの内の上位の64ビットのパラレルデータが初期設定される。疑似乱数発生回路1310、1320は、設定されたデータの排他論理和を演算して、1ビットデータを生成し、さらに、1ビット分だけシフトした上で、排他論理和を演算して、次の1ビットデータを生成するというように、64ビットのシリアルデータを出力する。疑似乱数発生回路1310、1320の出力するシリアルデータは、論理和回路1330によって演算され、64ビットのシリアルデータとして出力される。

【0041】即ち、変換部1300は、入力した128ビットのデータを、2分割した上で、それぞれのデータに基づいて、所定の論理演算を行い、64ビットのデータとして出力するものである。入力するデータが、128ビットよりも少ない場合には、所定の冗長ビットを付加して、128ビット構成とし、128ビットよりも多い場合には、所定のビットを削除して、128ビット構成とすることができる。また、ビット構成は、128ビットから64ビットに変換するだけでなく、他の任意ビットの変換を行うようにすることができる。また、シフトレジスタを用いた疑似乱数発生回路以外のハード構成を持つものでもよく、さらに、ソフトウェアにより同様の機能を達成するものであってもよい。

【0042】本実施形態においては、従来から用いられている固定の認証鍵1270以外に、逐次書き換えられる履歴情報1210、1220、1230、1240、1250、1260を用いて、新たな認証鍵を生成するようにした点に特徴があるものである。

【0043】次に、図5を用いて、本発明の一実施形態による携帯電話システムにおける認証実行手順について説明する。図5は、本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタにおける認証実行手順を示すフローチャートである。

【0044】図5に示す例では、基地局2100に接続しようとしている携帯端末1000が、接続を許された正当な携帯端末であるか否かを認証するものである。

【0045】ステップ501において、携帯端末1000のユーザが、相手先の電話番号を押し電話をかける。携帯端末1000は、記憶部1200に記憶されている携帯端末識別番号を、管理センタ2300へ基地局2100経由で転送する。

【0046】ステップ521において、管理センタ2300は、転送されてきた携帯端末識別番号が前もって登録されているか確認を行い、登録されている場合は、転送されてきた携帯端末識別番号に対応する履歴情報及び固定の認証鍵を記憶部2320から検索する。

【0047】次に、ステップ502において、携帯端末1000の変換部1300は、また、ステップ522において、管理センタ2300の変換部2320は、図4において説明したようにして、新しい認証鍵を生成す

(6)

特開平10-164656

10

る。

【0048】ステップ523において、管理センタ2300の制御部2310は、携帯端末1000に対して、基地局2100経由で認証用データAを転送する。

【0049】ステップ503において、携帯端末1000の制御部1100は、ステップ502において生成した新しい認証鍵に基づいて、管理センタ2300から送られてきた認証用データAを、認証応答aに変換する。この変換自体は、従来から行われている認証用データAを、個々の携帯端末に予め設定されている認証鍵を用いて認証応答aに変換するのと同様である。本実施形態においては、変換に使用する認証鍵が、従来とは相違するものである。

【0050】同様にして、ステップ524において、管理センタ2300の制御部2310は、ステップ522で生成した新しい認証鍵に基づいて、認証用データAを認証子a'に変換する。

【0051】次に、ステップ504において、携帯端末1000の制御部1100は、無線回路部1500を経由して、認証応答aを、管理センタ2300へ基地局2100経由で転送する。

【0052】ステップ505において、携帯端末1000は、サービス応答待ちになる。

【0053】一方、ステップ525において、管理センタ2300の制御部2310は、携帯端末1000から転送されてきた認証応答aと、ステップ524において管理センタ2300自身で作成した認証子a'を比較する。

【0054】ステップ526において、管理センタ2300は、ステップ525における比較結果が一致するか否かを判断する。

【0055】一致した場合には、ステップ527において、管理センタ2300は、交換制御部2200に通話を許可し、一致しない場合には、ステップ528において、管理センタ2300は、交換制御部2200に通話を拒否する。

【0056】なお、携帯端末の個々の過去の履歴情報や携帯端末個々に割り当てられている識別番号を格納してある記憶部の内容をダウンロードして不正を行うような場合もありうるので、そのような場合の対策としては、図2に、破線で示す不正開放検出手段1280と消去回路1290を設ければよいものである。不正開放検出手段1280は、例えば、携帯端末の筐体を止める複数のビスを所定の順番で緩めない、電源電圧の信号を出力するものである。消去回路1290は、不正開放検出手段1280の信号に基づいて、例えば、EEPROMから構成される記憶部1200の記憶内容を消去するようにすればよいものである。

【0057】なお、以上の説明では、記憶部に記憶された履歴情報の書換は、各通話の終了毎に行うものとした

が、複数回の通話毎に行うようにしてもよく、また、携帯端末のユーザの要求に応じて行うようにしてもよいものである。

【0058】本実施形態によれば、従来の個々の携帯端末に予め割り当てられている認証鍵に加えて、逐次書き換えられる履歴情報を用いて、新しい認証鍵を生成するようにしているため、不正使用を防止し得るものとなる。

【0059】次に、図6及び図7を用いて、本発明の第2の実施形態による携帯電話システムについて説明する。最初に、図6を用いて、本発明の第2の実施形態による携帯電話システムの監視制御部について説明する。図6は、本発明の第2の実施形態による携帯電話システムの監視制御部のブロック図である。

【0060】本実施形態においても、携帯電話システムの全体構成は、図1に示したものと同様である。本実施形態においては、図1に示した監視制御部2400を用いて、不正使用をチェックするようにしているものである。

【0061】監視制御部2400は、制御部2410と、記憶部2420と、インタフェース部2440と、時計2450とから構成されている。

【0062】制御部2410は、監視制御部2400の全体の制御や、記憶部2420のアクセス及び通話料金や通話位置によって携帯端末の不正使用を検出するものである。記憶部2420は、携帯端末ユーザの通話料金の上限、ユーザの前回の通話位置及び通話終了時間等を格納する。

【0063】インタフェース部2440は、交換制御部2200との接続を制御する。時計2450は、時間を計測し、記憶部2420に記憶される履歴情報の中の前回の通話時間等の時間に関する情報の基準となる時間信号を発生している。

【0064】なお、各構成要素は、例えば、DSP、CPU、ROM、RAM各種CMOS等の電子デバイスにて実現可能である。

【0065】監視制御部2400は、携帯端末ユーザの通話料金や通話位置によって携帯端末の不正使用を検出する装置であり、管理センタ2300は携帯端末の認証を行うだけの装置である。監視制御部2400と管理センタ2300は、別々の装置であっても良いし、同一の装置であっても良い。

【0066】次に、図7を用いて、本発明の第2の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順について説明する。図7は、本発明の第2の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順を示すフローチャートである。

【0067】ステップ700において、監視制御部2400の記憶部2420に、ユーザ毎に、月毎の通話料金の上限及び日毎の通話料金の上限を登録する。



(7)

特開平10-164656

11

【0068】次に、ステップ701において、監視制御部2400の制御部2410は、日毎及び月毎に通話料金を監視し、ユーザ毎の通話料金が予め登録しておいた通話料金の上限を越えているかチェックする。

【0069】ステップ702において、監視制御部2400の制御部2410は、日毎及び月毎に通話料金が、ユーザ毎の通話料金が予め登録しておいた通話料金の上限を越えているか否かを判断し、越えていない場合には、正当な使用であると判断して、ステップ702に戻る。越えている場合には、不正な使用であるとして、ス

テップ704に進む。

【0070】ステップ704において、監視制御部2400の制御部2410は、管理センタ2300へ、このユーザの携帯端末使用停止命令のコマンドを送る。

【0071】次に、ステップ705において、管理センタ2300は、このユーザの携帯端末使用停止命令のコマンドを受け取ると、ユーザの携帯端末識別番号及び認証鍵を抹消する。この操作によって、ユーザの携帯端末は、認証が正当に行われなくなるため、携帯端末の使用ができなくなる。

【0072】なお、以上の説明では、正当使用者が、料金の上限を越えて使用する場合にも、ユーザの携帯端末識別番号及び認証鍵が抹消されることになるので、かかる事態を避けるためには、ステップ703において、上限を越えていると判断された場合には、予め、携帯端末のユーザに対して、上限値を越えた旨通知するようにしてもよいものである。

【0073】本実施形態によれば、監視制御部によって、通話料金をチェックすることにより、容易に、不正通話を防止し得るものとなる。

【0074】次に、図8を用いて、本発明の第3の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順について説明する。図8は、本発明の第3の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順を示すフローチャートである。

【0075】なお、本実施形態においても、携帯電話システムの全体構成は、図1に示したものと同様であり、また、監視制御部2400の構成は、図6において説明したものと同様である。本実施形態においては、図6に示した監視制御部2400を用いて、不正使用をチェックするようにしているものである。

【0076】ステップ801において、監視制御部2400の制御部2410は、通話開始時もしくは通話中もしくは通話終了時に、時計2450によって得られる時刻情報と、携帯端末を使った位置特定システムによって得られる位置情報を記憶部2420へユーザ別に格納する。

【0077】次に、ステップ802において、監視制御部2400の制御部2410は、通話毎に通話開始時も

12

しくは通話中もしくは通話終了時に、時計2450によって得られる時刻情報と、携帯端末を使った位置特定システムによって得られる位置情報を得て、今回の時刻情報と前回の時刻情報との差が予め設定した一定の時刻T以内であり、かつ、今回の通話位置と前回の通話位置との差が予め設定した一定の距離D以上離れているかをチェックする。

【0078】ステップ803において、監視制御部2400の制御部2410は、ステップ802におけるチェック結果を判断して、YESであれば、不正な使用であるとして、ステップ804に進み、NOであれば、正当な使用であるとして、ステップ802に戻る。

【0079】ステップ803において、YESである場合は、例えば、1月1日の午前9時に携帯端末が、東京にある基地局の管内で使用され、同一の識別番号を有する携帯端末が、同日の午前9時5分に、北海道にある基地局の管内で使用された場合等が該当する。即ち、通常の携帯端末の使用状況からして、時間的、空間的に、同一の識別番号を有しながら、異なる携帯端末が使用されたような状況を識別するようにしている。ここで、予め設定しておくべき時刻情報Tと位置情報Dは携帯端末全てのユーザに共通であっても、個々に異なってもよい。

【0080】ステップ804において、監視制御部2400の制御部2410は、管理センタ2300へ、ユーザの携帯端末使用停止命令のコマンドを送る。

【0081】次に、ステップ805において、管理センタ2300は、ユーザの携帯端末使用停止命令のコマンドを受け取ると、管理センタ2300の記憶部2320からこのユーザの携帯端末識別番号及び認証鍵を抹消する。この操作によって、ユーザの端末認証が正当に行われなくなるため、携帯端末の使用ができなくなる。

【0082】なお、正当使用者に対しては、携帯端末識別番号及び認証鍵を抹消した旨を通知する。

【0083】本実施形態によれば、監視制御部によって、通話開始時間及び通話位置をチェックすることにより、容易に、不正通話を防止し得るものとなる。

【0084】

【発明の効果】本発明によれば、不正通話を防止し得るものとなる。

【図面の簡単な説明】

【図1】本発明の一実施形態による携帯電話システムのブロック図である。

【図2】本発明の一実施形態による携帯電話システムにおいて用いる携帯端末のブロック図である。

【図3】本発明の一実施形態による携帯電話システムにおいて用いる管理センタのブロック図である。

【図4】本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタ内部の変換部のブロック図である。

(8)

特開平10-164656

13

【図5】本発明の一実施形態による携帯電話システムにおいて用いる携帯端末及び管理センタにおける認証実行手順を示すフローチャートである。

【図6】本発明の第2の実施形態による携帯電話システムの監視制御部のブロック図である。

【図7】本発明の第2の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順を示すフローチャートである。

【図8】本発明の第3の実施形態による携帯電話システムの監視制御部における携帯端末の不正使用の検出手順を示すフローチャートである。

【符号の説明】

1000…携帯端末

1100…制御部

\* 1200…記憶部

1300…交換部

1310, 1320…疑似乱数発生回路

2100…基地局

2200…交換制御局

2300…管理センタ

2310…制御部

2320…記憶部

2330…交換部

10 2400…監視制御局

2410…制御部

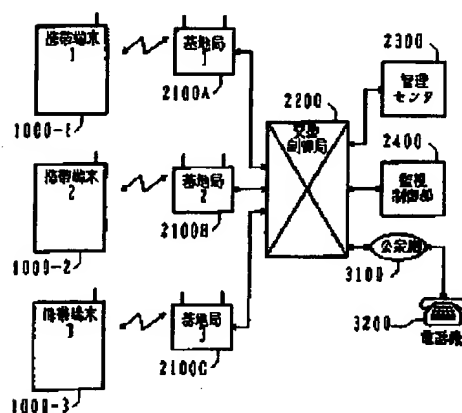
2424…記憶部

3100…公衆網

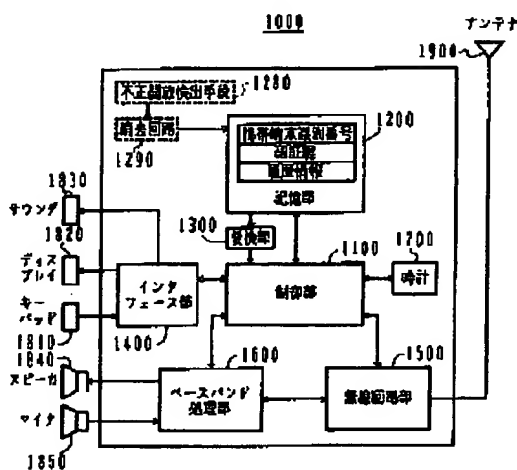
\* 3200…電話機

14

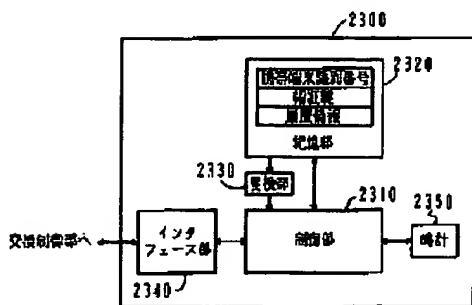
【図1】



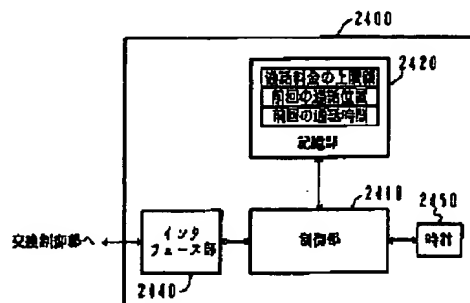
【図2】



【図3】



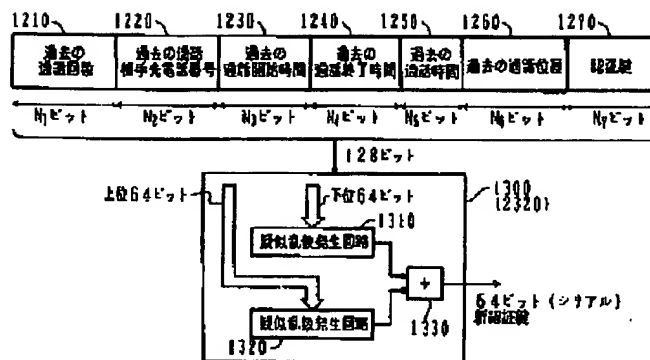
【図6】



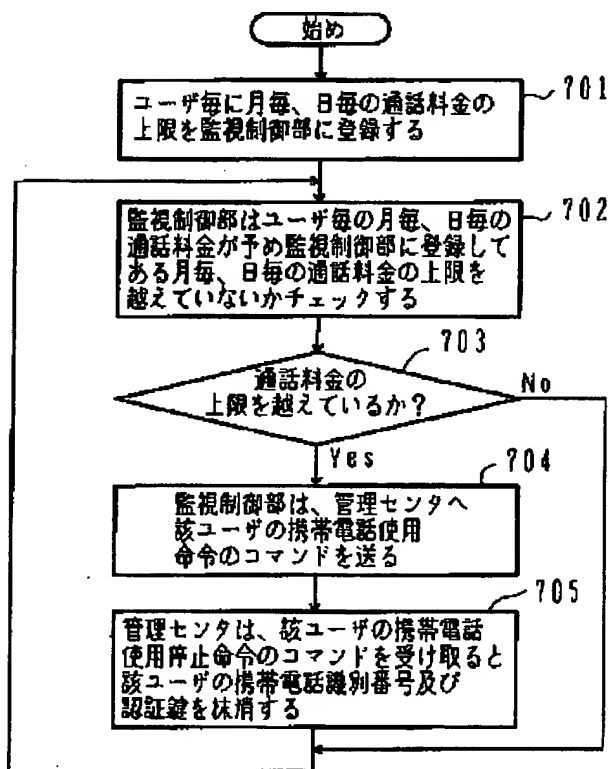
(9)

特開平10-164656

【図4】



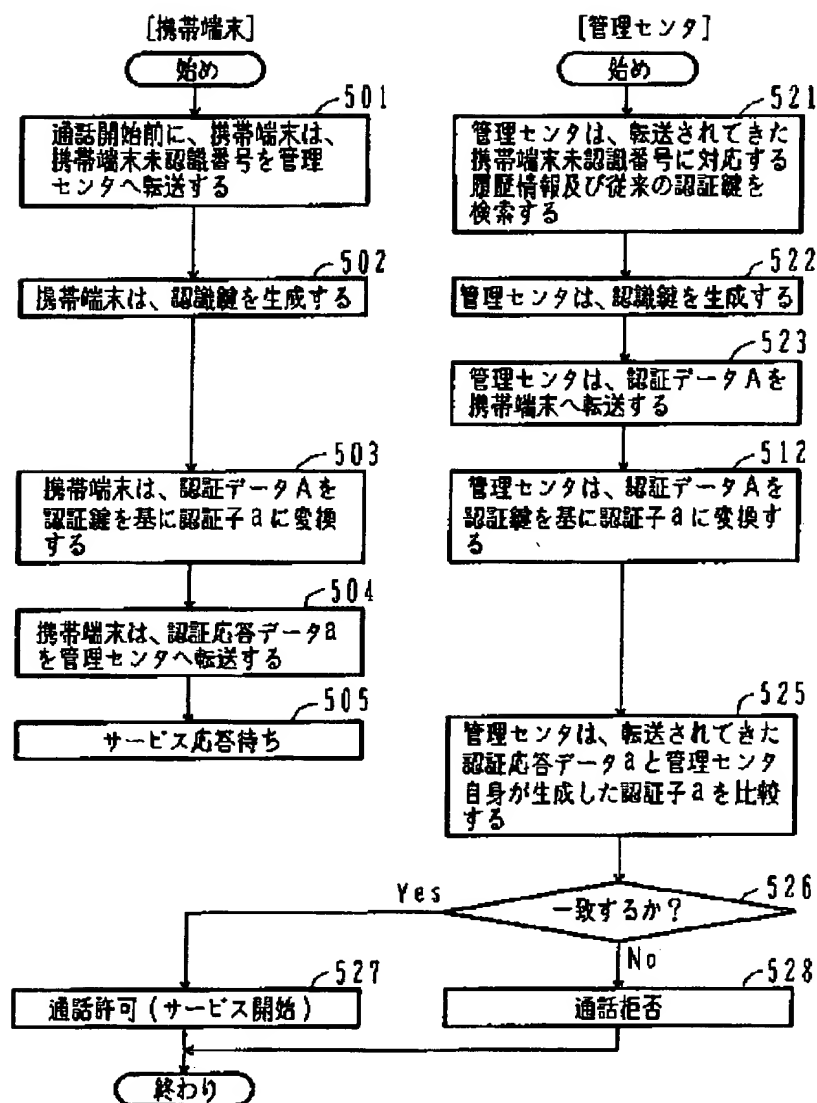
【図7】



(10)

特開平10-164656

【図5】



(11)

特開平10-164656

【図8】

